COUNTERFEIT DETERRENCE SYSTEM

Related Application Data

The present application is a continuation-in-part of copending provisional application 60/112,955.

The subject matter of the present application is related to that disclosed in the following, commonly-owned, copending applications: 09/127,502, filed 7/31/98; 09/099,864, filed 6/18/98; 09/074,034, filed 5/6/98; 09/287,940, filed 4/7/99; 09/234,780, filed 1/20/99; 09/185,380, filed 11/3/98, and 08/746,613, filed 11/12/96. WO9953428, WO9936876, and WO9743736 are laid-open counterparts to certain of the foregoing.

The present subject matter more generally relates to digital watermarking as typified, e.g., by the assignee's issued patents: 5,721,788, 5,768,426, 5,636,292, 5,841,978, 5,832,119, 5,745,604, 5,822,436, 5,841,886, 5,809,160, and copending applications 08/746,613, filed 11/12/96, 09/452,023, filed 11/30/99, entitled Watermark Detection Using a Fourier Mellin Transform, and 09/452,022, filed 11/30/99, entitled Method and System for Determining Image Transformation.

To provide a comprehensive disclosure, without unduly lengthening this specification, the disclosures of the foregoing patents and applications are incorporated herein by reference.

Background

The strong growth of high quality personal computing and consumer imaging systems requires an equally strong response to the counterfeit threat that these systems represent. A requirement to deter this counterfeit threat is to arm professional and consumer computer systems with the ability to recognize and respond to banknotes and other security documents (e.g., passports, visas, other immigration documents, postal stamps, stock certificates and other financial instruments, travelers checks, other checks, concert/event tickets, lottery tickets, etc.). This is no simple task, since the solution must be acceptable to a very diverse and competitive group of commercial manufacturers.

Detailed Description

A counterfeit deterrence system according to one embodiment of the present invention provides an effective and rapidly deployable global solution to this growing digital counterfeiting problem. The system provides a network of security document detectors in the personal computer infrastructure. These detectors create multiple intervention points in personal computers and related peripherals. Positive detection of a security document at any of these points triggers a predetermined counterfeit deterrence action.

Security document detection relies on a special digital watermark, termed an Anti-Counterfeiting System (ACS) mark, which is added to security document designs. Such marking does not distract from the aesthetics of the security document, yet is readily and reliably detected during typically operations on a personal computer system. The ACS marks can be added to existing security document designs without changing the artwork (e.g. by pre- or post-processing the note to provide texture- or ink-markings). New designs can incorporate the watermarks as an integral part of their artwork.

The preferred counterfeit deterrence system is capable of several deterrence actions in response to detection of a security document. These range from issuing warnings, to preventing certain operations, to scarring security document images -- all designed to substantially deter creation of passable counterfeits.

The illustrative system's intervention strategy prevents the acquisition and printing of security document images, while providing artists with a central resource to obtain approved images for use in marketing, communications, and other legitimate uses. These approved images can be controlled and distributed without certain key security features, with additional special security features, and offered in a way that balances the use of security documents as a symbol of country and commerce, without increasing the risk of counterfeiting. The result is eventual removal of unauthorized security document images from the desktop computing environment (provided necessary assistance is provided by issuing entities and computer equipment vendors; the latter may be required by legislation). (In other fields, recognition of an image by reference to a watermark may trigger other actions, such as commerce opportunities.)

Detectors are deployed both in hardware and software. For example detectors are deployed in image editing applications to intervene in scanning, file open, and file save operations, and in various device drivers. These initial locations can be supplemented to include other processing points, such as internet browsers, operating system, multi-function desktop peripherals, etc., etc.

Intervention is augmented by a covert tracing system, which can be an integral part of the counterfeit deterrence system. As detailed in application 09/185,380, covert tracing serves to record suspected counterfeiting operations in multiple locations on the offending personal computer in a way that is intentionally obscured from the user. Law enforcement can use special tools to recover the covert audit trail, providing a means to corroborate a suspected offense. This system greatly increases the risk to the counterfeiter, as they will never be sure that all evidence of their counterfeiting activities has been removed from their equipment. If desired, resellers of used computers (or manufacturers processing equipment returned through the retail channel) could scan the computers/peripherals for potential illicit uses.

Embedder

A counterfeit deterrence system according to one embodiment of the present invention includes an embedder, one or more detectors, and (optionally) a covert tracing system. The embedder serves to embed an ACS Mark into a security document.

The ACS mark can take various forms -- both visible and imperceptible -- as detailed in the cited patents and applications.

The ACS mark embedder is a set of software programs designed to assist the user in application of ACS marks to security documents designs in the pre-press stage of development, either through universal application to the design, or application to a single plate or portion of a plate. An illustrative embedder runs under the Windows NT operating system and performs various functions, including receiving high-resolution security document image data, rasterizing vector designs, creating masks for those images (i.e. defining the areas of a plate that are to receive an ACS mark, and at what respective intensities), embedding ACS marks in rasterized image data, and transferring files to and from the prepress system. (Counterpart operations can

likewise be performed for ACS marks applied as texturing, with or without ink.) In one embodiment, the embedder is a stand-alone group of programs. In another, it is a suite of tools that integrates seamlessly with designer tools, such as the Barco Fortuna system (e.g. using that system's TIFIT file export function). In either case, the ACS marks can be designed-in as part of the original artwork, or can be added-in after the original artwork has been completed. The output is typically produced in either TIFF or PNG form.

The ACS mark can be a single bit (i.e., "do not copy"), but more typically comprises a plural-bit payload (e.g., 2 – 128 bits). Data conveyed in the payload can include, for a banknote, the denomination and country of issuance. The payload can also include a reserved area that can be encoded differently, as particular needs arise. For example, notes can be serialized. Or notes can be marked for special purposes (e.g. circulation control) or to facilitate statistical studies (e.g. geographic dispersal studies for groups of notes issued from different banks).

The embedder can work on a per-plate/film basis. (Plural plates/films are commonly used to print a single security document.) The image for an exemplary plate is 37,500 pixels by 75,000 pixels, and is printed at a resolution in excess of 2500 dpi (e.g. 10,000 dpi).

The embedder desirably employs traditional user interface elements to facilitate the different operations. For example in embedding, an illustrative user interface permits the operator (1) to select one or more areas of a plate for application of an ACS mark, (2) to select the intensity of the ACS mark, (3) to add ACS marked background tints to the design, to (4) to manage marking of designs in which there are common design elements between different notes, etc., etc.

Background tinting is discussed in the related applications (e.g. 09/127,502, filed July 31, 1998) and refers to subtle, visible patterning that encodes watermark data. In one embodiment, the patterning is tiled (i.e. repetitive). In another, the patterning is scrambled using one of various known image manipulation/encryption techniques so that the same data is conveyed, but the patterning no longer has a repetitive appearance. In the cited application, the preferred tinting took the form of a weave pattern of fine lines. In other embodiments, tinting not based on weave patterning can be used -- e.g. other patterning that results in the desired luminance/reflectance changes can be employed. Such tinting can be applied to clear areas of the document, such as

over the top of traditional paper watermarks where printing is usually limited so as to allow viewing of the paper watermark.)

Reference was made in the prior applications to the use of a grid pattern. For robustness and security reasons, the embedder may have the capability of incorporating multiple grid patterns into a single design. The embedder may also have the capability to vary the ACS mark intensity from region to region within a single plate or film.

ACS marks can be applied in regions of continuous tone in the security document artwork. If the area is devoid of ink (i.e. the note in that region shows just the unprinted substrate), fine droplets of ink (e.g. less than 100 microns in diameter) can be scattered through the region to define the necessary changes in luminance/reflectance, without detracting from the aesthetics of the design. If the area has a uniform region of ink, small points devoid of ink (again, typically less than 100 microns, e.g. 30-50 microns) can be incorporated in the design to effect the intended luminance/reflectance change. In both cases, droplets or points of non-uniform size can be used so as to minimize visibility.

Although the detailed embedder performs the embedding in the pixel domain, the tool could also support application of the ACS marks directly to vector design files, without the need to first convert the design to raster files.

If desired, a validation tool can be provided with the embedder to read and examine the payload and strength of an ACS mark in a digital image or in a scan of a marked document. The results of such a tool can be used in a design environment in which tradeoffs between visibility and robustness are iteratively balanced.

Detector

An illustrative ACS mark detector is a software development kit (SDK) designed for integration into software applications and control software including image editing applications, TWAIN drivers, scanner device drivers, printer device drivers, and other intervention points. In an exemplary environment, the SDK is a C/C++ callable library that includes a programming interface to the detector for easy integration into various software products. The detector may support various different color formats (e.g. RGB, CMYK, etc.).

In other embodiments, the detector takes the form of hardware, e.g. an ASIC, PLA, etc.

Audit trail functionality (discussed below) can be integrated into the detector, causing detection of an ACS mark to trigger writing of covert audit records, e.g. in the host computer. The detector may also be responsive to other watermarks (e.g., the commercial digital watermark that can be embedded using Adobe Photoshop or using other image editing software available from other vendors). The detector(s) can be deployed at various intervention points, including scanner hardware, scanner driver, operating system, image editing application, printer driver, printer hardware, internet browser, communications port, etc.

Desirably, the detector is fully integrated with the software of which it forms a part, to prevent trivial work-arounds, such as removal of plug-ins.

When a detector senses security document image data, it can intervene in various ways. In one embodiment, the detector intervenes with a dialog box advising the user:

> *"This application does not support unauthorized <scanning, editing, printing, etc., as applicable> of controlled security documents. To obtain images for legitimate use, select 'Get Image' below, or go to www.imagedistribution.com."*

This dialog box includes a "Get Image" button that launches/directs a web browser resident on the computer to a web site authorized by the document issuer, from which substitute legitimate security document images are available for downloading. The substitute images appear -- on first inspection -- to be authenticate security document images, and are sufficiently close to satisfy all legitimate uses for security document imagery (e.g. for use in advertising, etc.) but on closer inspection are evidently illegitimate (e.g. they may be low resolution, front-only, and have certain key security features removed). Slightly different substitute images can be provided to each user (e.g. each image can have different tracking information embedded as a digital watermark). Registration and pre-authorization may be required for users who request the substitute images, and different security/authentication techniques can be employed to assure that accurate registration data is obtained.

By this arrangement, it may eventually be possible to remove all unauthorized security document images from circulation, including stock photography and numismatic uses.

The just-described web site additionally provides additional relevant information. For example, it can include warnings regarding counterfeiting and illegal reproduction of security documents, specific to that country. It can also provide guidelines for legitimate use of security document images (e.g. required size/color, required registration and pre-authorization, etc.)

The dialog box further includes a "Cancel" button that simply aborts the operation <scanning, printing, file opening, etc.> that triggered the detector response.

Another detector intervention is for the detector to substitute its own substitute data for the security document data. Scanning of a security document can result, for example, in image data corresponding to play money. Likewise for printing.

In the case of a detector associated with the printer, the intervention response can be visual scarring of the image with the words "Copy" clearly repeated across the printed image.

To cope with the problem of legacy equipment, ACS mark detection capability can be provided by updated device drivers. Updated device drivers are commonly installed when a new application employing the device is installed, or an updated operating system is installed. On-line updates are also available for many programs; ACS mark compliant drivers can be installed via such on-line mechanisms as well. By such approaches, ACS mark capability is extended even to equipment that was released before deployment of the counterfeit deterrent system.

The detector functionality can be tailored to the environment in which it is used, and the computing resources available to it. For example, in the environment of a printer, the detector may not need to concern itself with security documents that are printed at 150% normal size; such notes would never be passable. In contrast, detectors in image editing equipment should be robust against all manner of scaling.

Outside the PC realm, ACS mark detectors can be used in various security document reading/authenticating applications, and their functional requirements can depend accordingly. In vending machines, for example, the feed mechanism limits rotations of the security document, and user-instructions can require that the note be fed from a predetermined end. In such environment, scale and rotation are effects that can almost be disregarded. Similarly in banknote counting equipment, and in quality assurance testing apparatuses used by security document printers.

Covert Tracing

The covert tracing function (e.g. the writing of hidden audit trail data in response to detection of security document data) is fully detailed in application 09/185,380, so that disclosure is not repeated here. Suffice to say that any detection of security document image data can trigger storage of one or more records that may include any or all of: payload of the detected ACS mark, data/time the operation was performed, computer type, operating system and version number, user ID, printer type, printer driver version, scanner type, and scanner driver version.

In an illustrative embodiment, the covert tracing function is invoked not just when security document data is sensed, but also when an attempt is made to patch or attack the detector software or functionality. Those skilled in the computer arts will recognize various code security techniques and other approaches by which such tampering can be detected.

Miscellaneous

Patent 5,841,886 discloses a self-authenticating identification document in which an image on the document is steganographically encoded to correspond in a predetermined manner with human-perceptible information on the document. For example, the name of the owner of the card is both steganographically encoded in an image of the owner on the card, and is also textually printed on the card.

In related embodiments, the steganographically-embedded data need not -- itself -- match the human-perceptible information on the document (e.g. the text). Instead, the correspondence can be effected through, e.g., a remote database. In such example, the embedded data can be an index into a remote database. A record in the database identified by this index can contain information on the card owner, including the card-owner's name. Thus, to authenticate the user, the index is steganographically decoded from the image, and the database then checked to confirm that the owner name corresponding to that index matches the owner name printed on the card.

The same principles can be applied to documents other than identification documents. Stock certificates and other security documents can be steganographically encoded in such

manners as an aid to authentication. In the case of a stock certificate, the steganographic encoding can be accomplished by any of the security document embedding techniques discussed in the cited applications (e.g. line width modulation, etc.).

Conclusion

Having described and illustrated the principles of our invention with reference to an illustrative embodiment and several variations thereon, it should be recognized that the invention can be modified in arrangement and detail without departing from such principles.

For example, while the invention has been illustrated as focusing on PC-based counterfeiting, the same detectors and similar intervention responses can be employed with color photocopiers.

Similarly, while the invention has been illustrated with reference to digital watermark-based recognition of documents, other document recognition techniques can be employed in other embodiments. For example, there is a vast literature on photocopiers that recognize banknotes by reference, e.g., to spectral characteristics, visible pattern recognition (e.g., Bank of Japan seal), the word CONFIDENTIAL, etc. Bar codes and glyphs are among many other indicia by which protected documents may similarly be distinguished. Any such recognition technology can be employed, e.g., to launch a web browser providing the user with a suitable response (e.g., advising the user of applicable limitations, making available substitute images, etc.).

Similarly, it should be recognized that, guided by the foregoing teachings, various watermarking, decoding, and anti-counterfeiting technologies can be substituted for, and/or combined with, the elements detailed above to yield advantageous effects. Other features disclosed in the cited patents and applications can similarly be employed in embodiments of the technology detailed herein. (Thus, this specification has not belabored application of each of the techniques disclosed in the cited patent documents -- e.g. use of neural networks for detectors -- to the present subject matter since same is fairly taught by reading the present disclosure in the context of the earlier patent documents.)

Still further, it will be recognized that the technology detailed above may also be used for non-security applications, e.g., recognizing images, video, or audio being processed on a user's computer as belonging to a certain class, and presenting the user with a web page relating to that class of object. Commerce opportunities may thereby be made available to the user.

While this specification has focused on a "system" incorporating an embedder, ACS marked security documents, and various detectors (including covert tracing features), it will be recognized that the individual components and sub-combinations are patentable independently from the complete system.

In view of the diverse embodiments to which the principles of our invention may be applied, it should be understood that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such embodiments as may come within the scope and spirit of the following claims, and equivalents thereto.